UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/090,718	03/04/2002	Martin Hurich	10191/2275	4797

26646 7590 06/02/2008

KENYON & KENYON LLP
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	PAPER NUMBER
2136	
MAIL DATE	DELIVERY MODE
06/02/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/090,718	HURICH, MARTIN	
	Examiner	Art Unit	
	DAVID CERVETTI	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 March 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12 and 15-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12 and 15-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 March 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed March 11, 2008, have been fully considered.

2. Claims 1-12 and 15-19 are pending and have been examined. Claims 13 and 14 have been cancelled.

Response to Amendment

3. Regarding Applicant's argument that "each and every claim feature is identically described or contained in a single prior art reference", Examiner respectfully submits that:

4. **TO ANTICIPATE A CLAIM, THE REFERENCE MUST TEACH EVERY ELEMENT OF THE CLAIM** "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). >"When a claim covers several structures or compositions, either generically or as alternatives, the claim is deemed anticipated if any of the structures or compositions within the scope of the claim is known in the prior art." *Brown v. 3M*, 265 F.3d 1349, 1351, 60 USPQ2d 1375, 1376 (Fed. Cir. 2001) (claim to a system for setting a computer clock to an offset time to address the Year 2000 (Y2K) problem, applicable to records with year date data in "at least one of two-digit, three-digit, or four-digit" representations, was held anticipated by a system that offsets year dates in only two-digit formats). See also MPEP § 2131.02.< "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim, but this is not an *ipsissimis verbis* test, i.e., identity of terminology is not required. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990). Note that, in some circumstances, it is permissible to use multiple references in a 35 U.S.C. 102 rejection. See MPEP § 2131.01." MPEP 2131

5. Regarding Applicant's argument that the prior art, namely Takaragi, does not disclose the equation, the equation is irrelevant, since Takaragi teaches what the equation tries to accomplish, encrypt and decrypt information. Further, the disparaging remarks about the reference map to what the claim language does, namely performing an operation (basic) on bytes of information. With the richness of the English language, perhaps an explanation of what the equation does should replace said equation in the body of the claim. It is further noted that the equations do not add anything to the alleged "basic and fundamental binary operations" disclosed by Takaragi. Further,

according to the specification, the operations of the equations are nothing more, nothing less, than rotation to the left and rotation to the right, and exclusive OR (see page 5), accordingly, Takaragi's operations of "cyclically shifting and x-OR operations" (see previous Office Action) correctly map to the claimed subject matter. In other words, the equations encrypt by rotating to the left and then xoring, and decrypt by xoring and then rotating to the right. **Applicant's arguments are not persuasive.**

6. Regarding Applicant's argument about "no byte-wise allocation between input and output data occurs", Examiner respectfully points out that the cited portion further advances the office action's point, since a 64-bit input data and a 32-bit input data (96-bit input data) is ***expanded*** to 128-bit output data. There is a difference of 32 bits, i.e. there is "no byte-wise allocation between input and output data occurs". **Applicant's arguments are not persuasive.**

7. Regarding the argument that the key is not part of the unit in Takaragi, Examiner again, respectfully submits, that considering Takaragi's text, in context, and fig. 19, in context, fig. 19 is a function that resides in the decoder of fig. 18, the key is input to the function, not to the decoder. Therefore, at the point of feeding the key to the decoding function, the key can be interpreted as residing in the decoder which is mapped to the control unit, then, Takaragi still anticipates the claim. **Applicant's arguments are not persuasive.**

8. Assuming arguendo none of the features claimed are met by Takaragi, Applicant seems to admit or agree that Takaragi at the very least provides an allegedly basic architecture to implement the invention. Under this hypothetic scenario, making

changes to the "basic" Takaragi invention would have been obvious to someone of ordinary skill in the art, i.e. encrypting data, transmitting it, and decrypting it according to a given algorithm.

Claim Rejections - 35 USC § 102

9. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

10. Claims 1-12 and 15-19 are rejected under 35 U.S.C. 102(b) as being anticipated by Takaragi et al. (US Patent 6,141,421, hereinafter Takaragi).

Regarding claims 1 and 7, Takaragi teaches

- a method of data encryption in programming of a control unit comprising:
- encrypting a complete stream of data to be transmitted in a programming unit using a first key, wherein a byte by byte encryption of the complete stream of data is capable of being performed, and wherein no byte-wise allocation between input and output data occurs **(col. 5, lines 4-25, encryption and compression are performed together)**;
- transmitting the data that had been encrypted to the control unit via a data line **(col. 5, lines 4-25, encrypted and compressed message sent to receiver)**; and
- decrypting the data that had been encrypted in the programming unit using a second key provided in the control unit **(fig. 19, col. 14, lines 58-67, decoding process)**;

- wherein: successive bytes during encryption are provided with an index i, where i = 0,1,2,..., an encrypted byte n* is formed from an unencrypted byte n according to the following, a starting value n_{-1} being used for decryption and encryption **(col. 13, lines 45-67, first n bits)**:
- $n_{-1} \equiv S_0$
- $n_i^* = \left(n_i <<< \sum_{j=0}^{i} n_{j-1}^* \right) \oplus S_{h\left(\sum_{j=0}^{i} n_{j-1}^* \right)}$ **(col. 9, lines 30-45, cyclically shifting bits and exclusive OR operations)**
- an unencrypted byte n is formed from an encrypted byte n* according to the following:
- $n_i = \left(n_i^* \oplus S_{h\left(\sum_{j=0}^{i} n_{j-1}^* \right)} \right) >>> \sum_{j=0}^{i} n_{j-1}^*$ **(col. 9, lines 30-45, cyclically shifting bits and exclusive OR operations)**

Regarding claim 11, Takaragi teaches

- performing an encryption of a complete stream of data in accordance with a table and a hash function **(abstract, hash function)**, wherein a byte by byte encryption of the complete stream of data is capable of being performed, and wherein no byte-wise allocation between input and output data occurs **(abstract, input M, output longer)**;
- wherein: successive bytes during encryption are provided with an index i, where i = 0,1,2,..., an encrypted byte n* is formed from an unencrypted

byte n according to the following, a starting value n_{-1} being used for decryption and encryption **(col. 13, lines 45-67, first n bits)**:

- $n_{-1} \equiv S_0$
- $n_i^* = \left(n_i <<< \sum_{j=0}^{i} n_{j-1}^* \right) \oplus S_{h\left(\sum_{j=0}^{i} n_{j-1}^* \right)}$ **(col. 9, lines 30-45, cyclically shifting bits and exclusive OR operations)**
- an unencrypted byte n is formed from an encrypted byte n* according to the following:
- $n_i = \left(n_i^* \oplus S_{h\left(\sum_{j=0}^{i} n_{j-1}^* \right)} \right) >>> \sum_{j=0}^{i} n_{j-1}^*$ **(col. 9, lines 30-45, cyclically shifting bits and exclusive OR operations)**.

Regarding claim 15, Takaragi teaches

- a program code executable on a computing unit for performing an encryption of a complete stream of data in accordance with a table and a hash function **(abstract, hash function)**,
- wherein a byte by byte encryption of the complete stream of data is capable of being performed, and wherein no byte-wise allocation between input and output data occurs **(abstract, input M, output longer)**;
- wherein: successive bytes during encryption are provided with an index i, where i = 0,1,2,..., an encrypted byte n* is formed from an unencrypted

byte n according to the following, a starting value n_{-1} being used for decryption and encryption **(col. 13, lines 45-67, first n bits)**:

- $n_{-1} \equiv S_0$
- $n_i^* = \left(n_i <<< \sum_{j=0}^{i} n_{j-1}^* \right) \oplus S_{h\left(\sum_{j=0}^{i} n_{j-1}^* \right)}$ **(col. 9, lines 30-45, cyclically shifting bits and exclusive OR operations)**
- an unencrypted byte n is formed from an encrypted byte n* according to the following:
- $n_i = \left(n_i^* \oplus S_{h\left(\sum_{j=0}^{i} n_{j-1}^* \right)} \right) >>> \sum_{j=0}^{i} n_{j-1}^*$ **(col. 9, lines 30-45, cyclically shifting bits and exclusive OR operations)**.

Regarding claim 16, Takaragi teaches

- a program code executable on a computing unit for performing a decryption of a complete stream of data in accordance with a table and a hash function **(abstract, hash function)**, wherein a byte by byte decryption of the complete stream of data is capable of being performed, and wherein no byte-wise allocation between input and output data occurs **(abstract, input M, output longer)**;
- wherein: successive bytes during encryption are provided with an index i, where i = 0,1,2,..., an encrypted byte n* is formed from an unencrypted byte n according to the following, a starting value n_{-1} being used for decryption and encryption **(col. 13, lines 45-67, first n bits)**:

- $n_{-1} \equiv S_0$

- $n_i^* = \left(n_i <<< \sum_{j=0}^{i} n_{j-1}^* \right) \oplus S_{h\left(\sum_{j=0}^{i} n_{j-1}^* \right)}$ **(col. 9, lines 30-45, cyclically shifting bits and exclusive OR operations)**

- an unencrypted byte n is formed from an encrypted byte n* according to the following:

- $n_i = \left(n_i^* \oplus S_{h\left(\sum_{j=0}^{i} n_{j-1}^* \right)} \right) >>> \sum_{j=0}^{i} n_{j-1}^*$ **(col. 9, lines 30-45, cyclically shifting bits and exclusive OR operations)**.

Regarding claims 2 and 8, Takaragi teaches wherein the first key and the second key are identical **(col. 3, lines 25-50, DES algorithm)**.

Regarding claims 3 and 9, Takaragi teaches wherein the first key and the second key are not identical **(col. 16, lines 10-20, RSA algorithm)**.

Regarding claim 4, Takaragi teaches wherein each one of the first key and the second key includes a table that is accessed by a hash function **(col. 11, lines 35-55, hash function)**.

Regarding claim 5, Takaragi teaches wherein at least one of the first key and the second key is implemented in an electronic circuit **(fig 15, 1508, random number generator)**.

Regarding claim 6, Takaragi teaches wherein at least one of the first key and the second key is implemented in the form of a computer program **(fig. 13, col. 11, lines 35-55, output of hash function is used as work key)**.

Regarding claim 17, Takaragi teaches

- wherein there is no bit-wise allocation between input and output data **(abstract, input M, output longer)**:
- wherein: successive bytes during encryption are provided with an index i, where i = 0,1,2,..., an encrypted byte n* is formed from an unencrypted byte n according to the following, a starting value n_{-1} being used for decryption and encryption **(col. 13, lines 45-67, first n bits)**:
- $n_{-1} \equiv S_0$
- $n_i^* = \left(n_i <<< \sum_{j=0}^{i} n_{j-1}^* \right) \oplus S_{h\left(\sum_{j=0}^{i} n_{j-1}^* \right)}$ **(col. 9, lines 30-45, cyclically shifting bits and exclusive OR operations)**
- an unencrypted byte n is formed from an encrypted byte n* according to the following:
- $n_i = \left(n_i^* \oplus S_{h\left(\sum_{j=0}^{i} n_{j-1}^* \right)} \right) >>> \sum_{j=0}^{i} n_{j-1}^*$ **(col. 9, lines 30-45, cyclically shifting bits and exclusive OR operations)**.

Regarding claim 10, Takaragi teaches wherein the programming unit and the control unit each includes an electronic computing unit and a memory module that are linked together by a data bus **(col. 6, lines 1-13, apparatus)**.

Regarding claim 18, Takaragi teaches wherein there is no bit-wise allocation between input and output data **(abstract, input M, output longer)**.

Regarding claim 12, Takaragi teaches wherein the computing unit includes an electronic computing unit in a programming unit **(col. 6, lines 1-13, apparatus)**.

Regarding claim 19, Takaragi teaches wherein there is no bit-wise allocation between input and output data **(abstract, input M, output longer)**.

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAVID CERVETTI whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Tuesday and Thursday-Friday.

13. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

14. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David García Cervetti/
Primary Examiner, Art Unit 2136

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136